AMENDMENTS TO THE DRAWINGS:

The attached sheet of drawings includes changes to Fig. 3.

REMARKS

A substitute sheet of drawing is submitted to overcome the objection to the drawings.

The specification and claims have been amended so the American spelling of authorizing is used, to overcome the objection set forth in items 3 and 5 on pages 2 and 3 of the office action.

Claim 12 has been amended so it conforms to the specification and drawing of the application as filed. The specification as filed indicates session concentrator 100 includes non-volatile memory 102, for example a hard disk, that stores programs which implement the invention, in particular the program shown by the flow diagram of figure 3; see paragraph 0057 of the published application. Paragraph 0057 also indicates random access memory 103 stores the programs which are stored in memory 102. The specification as filed also indicates multiplexor 130 includes nonvolatile memory 202, for example, a hard disk, that stores programs which implement the invention, in particular the program shown by the flow diagram of figure 2; see paragraph 0043 of the published application. Paragraph 0043 also indicates random access memory 203 stores the programs which are stored in memory 202. Hence, the hard disks of memories 102 and 202 constitute the "computer readable medium arrangement" of claim 12 as amended while random access memories 103 and 203 constitute the "storage device arrangement" of claim 12. It is also to be understood that claim 12 is broad enough to include a single computer readable medium or a single storage device instead of the specifically described and illustrated arrangement including memories 102, 103, 202 and 203. Based on the foregoing, the objection to the specification set forth in item 4, page 2 of the office action has been overcome.

Applicants traverse the provisional double patenting rejection of claims 1, 11 and 12 (Group 1) of this application as being unpatentable over claims 1-14 (Group II) of co-pending application Serial Number 10/598595. The scope of Group I of the present patent application n°10/598,598 is <u>distinct</u> from the scope of Group II of the copending

patent application n°10/598,595.

The following comparative table indicates how the subject matter of the claims of Group I (left column) differ patentably from the claims of Group II (right column). The features for which the claimed subject matter is patentably identical (or substantially patentably identical) are indicated on the same row.

US Application n°10/598,598 (Group I)	US Application n°10/598,595 (Group II)
Claim 1: Method for access by a client to services provided by a service provider	*authenticating a client for access to at least one virtual network which allows the client to access the services of at least one service provider (claim 1)*
The client being able to transmit and/or receive information (...) via a telecommunication network,	*each virtual network being set up on a telecommunication network (claim 1)*
and a session concentrator which is able to transmit and/or receiving formation according to the point-to-point transport protocol,	*(no equivalence in the Group II)*
an access control protocol is used in the telecommunication network to control access to the services provided by the service provider,	*a predetermined access control protocol for access to the virtual network (claim 1)*
determining whether the client is conformed with the access control protocol,	*determining the compatibility of the client with a predetermined access control protocol for access to the virtual network (claim1)*
authorizing the client that does not conform to the access control protocol to access a network for non-conforming clients, the network for non-conforming clients being set up on the telecommunication network and allowing access to the session concentrator,	*(no equivalence in the Group II)*

establishing a session between the non-conforming client and the session concentrator according to a point-to-point transport protocol on the network for non-conforming clients,	*(no equivalence in the Group II)*
transferring, by the session concentrator, the information transmitted by the non-conforming client in the established session to a network for clients that conform to the access control protocol, the network for conforming clients being set up on the telecommunication network and allowing access to the services provided by the service provider, and reciprocally.	*(no equivalence in the Group II)*

Because claims 11 and 12 of Group I are substantially equivalent in scope to claim 1 of Group I, the arguments developed below are also applicable to claims 11 and 12 of Group I.

The comparative table indicates claim 1 of the present application n°10/598,598 is different in scope from the claims of Group II of the copending patent application n°10/598,595 because Group II does not include the following features of Group I:

the client being able to transmit and/or receive information according to a point-to-point transport protocol via a telecommunication network and a session concentrator which is able to transmit and/or receive information according to the point-to-point transport protocol,

the step of authorizing the client that does not conform to the access control protocol to access a network for non-conforming clients, the network for non-conforming clients being set up on the telecommunication network and allowing access to the session concentrator,

the step of establishing a session between the non-conforming client and the session concentrator according to a point-to-point transport protocol on the network for non-conforming clients, and

transferring, by the session concentrator, the information transmitted by the non-conforming client in the established session to a network for clients that conform to the access control protocol, the network for conforming clients being set up on the telecommunication network and allowing access to the services provided by the service provider, and reciprocally.

When the claims of Group I rely on the compatibility of a client with an access protocol for access to services of services providers, the claims of Group II rely on the compatibility of a client with an access protocol for access to a virtual network (to subscribe to services of service providers).

If the client is not compliant with the access protocol, the claims of Group I enable the non-conforming client to access a (second) network for non-conforming clients, this (second) network being set up on the (first) telecommunication network. Thus, the client can access a session concentrator which is in charge of sending information, according to a point-to-point protocol, transmitted by the client to a (third) network for conforming clients, also set up on the (first) telecommunication network, to enable the client to access services provided by service providers.

In Group II, if the client is not compliant with the access protocol, the data are transmitted between the non-conforming client and a subscribing system by an accreditation network enabling the subscribing of non-conforming client to services of service provider. If the non-conforming client subscribes to a service provider, the accreditation network carries out a transmission mechanism for transmitting an accreditation giving the client access authorization to the virtual network and information enabling to make the client compatible with the access control protocol. These features are in no way suggested in the claims of Group I.

Based on the above, the provisional double patenting rejection is incorrect.

Applicants traverse the rejection of claim 11 under 35 USC 101. Claim 11 includes the following limitations, which must be interpreted in accordance with 35 USC 112, paragraph 6:

(1) "means for determining whether or not the client conforms to the access control protocol" which reads on multiplexer 130, as set forth in paragraph 0046 of the published application;

(2) "means for authorizing the client that does not conform to the access control protocol to access a network for non-conforming clients" which reads on multiplexer 130, as set forth in paragraph 0046 of the published application; and

(3) "means for establishing a session between the client concentrator according to the point-to-point transport protocol on the network for non-conforming clients" which reads on an operation performed by processor 104 of session concentrator 100, as set forth in paragraph 0084 of the published application.

Multiplexer 130 includes CPU 200, nonvolatile memory 202, random access memory 203, client interface 205 and network interface 206; paragraph 0042 of the published application. Session concentrator 100 includes common bus 101, nonvolatile memory 102, random access memory 103, processor 104, server interface 105 and network interface 106; paragraph 0056 of the published application. Because the means plus function limitations of claim 11 are construed in accordance with 35 USC 112, paragraph 6, the foregoing limitations (1), (2) and (3) must be construed as the hardware elements of session concentrator 100 and multiplexer 130 or insubstantial differences thereof. Accordingly, claim 11 cannot be considered as being directed to non-statutory subject matter and the claim does, in fact, include the necessary physical articles or objects to constitute a machine within the meaning of 35 USC 101.

Applicants traverse the rejection of claims 1-3, 6, 11 and 12 under 35 USC 103(a) as being unpatentable over Hare et al. (US Patent Publication 2003/0167338) in view of Sobel et al. (US Patent 7,249,187) and the rejection of claims 4, 5 and 7-10 under 35 USC 103(a) as being unpatentable over Hare et al. in view of Sobel et al. and further in

view of Malik ("Network Security Principles and Practices," 15 November 2002, Cisco Press).

Hare et al. discloses an interconnection, using a point-to-point Protocol over Ethernet (PPPoE), between session concentrator *150* and clients *131, 132* which are able or unable to support PPPoE sessions (see *figure 1, §0006, §0020-0021).* When client *132*, which is unable to support the establishment of a PPPoE session, wants to access session concentrator *150*, an ATM (Asynchronous Transfer Mode) interface is implemented inside interconnection system *100* to create a virtual session *140* between gateway *110* (modem DSL, for example) and session concentrator *150*. Thus, client *132* can set up a communication with session concentrator *150*, via gateway *110*, even if client *132* is incompatible with the PPPoE protocol.

Despite the statements in the office action, Hare et al. does not disclose the following features of claim 1:

an <u>access control protocol</u> which is used in the *(first)* <u>telecommunication network</u> to control access to the services provided by the service provider; and

the steps of :

determining whether or not the client conforms to the <u>access control protocol</u> ;

authorizing the client that does not conform to the <u>access control protocol</u> to access a *(second)* <u>network for non-conforming clients</u>, the *(second)* <u>network for non-conforming clients</u> being set up on the (first) <u>telecommunication network</u> and allowing access to the session concentrator;

establishing a session between the non-conforming client and the session concentrator <u>according to a point-to-point transport protocol</u> on the *(second)* <u>network for non-conforming clients;</u>

transferring, by the session concentrator, the information transmitted by the non-conforming client in the established session to a *(third)* <u>network</u> for clients that conform to the <u>access control protocol</u>, the *(third)* <u>network</u> for conforming clients being set up on

14

the *(first)* telecommunication network and allowing access to the services provided by the service provider, and reciprocally.

Hare et al. does not disclose an access control protocol in a telecommunication network enabling access to services provided by a service provider. Instead, Hare et al. merely discloses a point-to-point protocol (PPPoE) in a telecommunication network. Furthermore, Hare et al. does not have three networks, namely a first telecommunication network on which are set up a second network for non-conforming clients and a third network for conforming clients.

A fortiori, there is nothing in Hare et al. that discloses or suggests implementation of a *(second)* network for non-conforming clients set up on the *(first)* telecommunication network, wherein this (second) network allows establishing a session between at least one non-conforming client and the session concentrator according to the point-to-point transport protocol. There is nothing in Hare et al. disclosing or suggesting a session concentrator that transmits client data to a *(third)* network for clients able to support the access protocol to allow such a client access to the services provided by the service provider.

When the method of claim 1 provides a technique for access to services based on two protocols and the relation of three networks (the second and third networks being set up on the first network), the Hare et al. technique is based on the use of an ATM interface enabling initiation of a virtual session (i.e. via a virtual communication channel) between a client and the session concentrator. The specification of the present application explicitly refers to that technique as the Prior Art technique; see paragraph 0004 of the published application. Such a technique is complex and difficult to implement, particularly if several clients subscribe to the same service provider and/or to the same service of the service provider.

As a consequence, Hare et al. is not relevant to the subject matter of the independent claims of the present application.

Sobel et al. relates to a system for enforcing computer network security policies. One of the goals of this reference is to enable a network administrator to ensure, for each client willing to access protected network *140* (e. g., applicant client *105*), a minimal access level to that network, by assigning to each client *105* either a protected network *140* or a restricted network *145* based on whether the client is compliant with the network's security policies *(see abstract ; col.2, lines 44-50).*

If the applicant client *105* is not in compliance with security policies implemented in protected network *140*, DHCP proxy server *110* intercepts the applicant client's request and assigns to it an address on the restricted network or no network address at all *(see col. 2, lines 3-10).*

The office action alleges Sobel et al. discloses the following features of claim 1:

an access control protocol used in the telecommunication network *(see col.5, lines 37-45)* ;

a determination as to whether or not a client conforms to the access control protocol *(col. 2, lines 46-50 ; col.4, lines 17-21);*

the client that does not conform to the access control protocol is authorized to access a network for non-conforming clients *(restricted network) (col. 2, lines 7-10).*

Although Sobel et al. deals with a technique for a client accessing a network for non-compliant clients (restricted network), nothing in this reference discloses or suggests (using the terms of claim 1):

<u>Preamble of claim 1:</u>

the method for access by a client to services provided by a service provider, the client being able to transmit and/or receive information <u>according to a point-to-point transport protocol</u> via a *(first)* telecommunication network and a session concentrator which is able to transmit and/or receive information <u>according to the point-to-point transport protocol</u>

Body of claim 1:

the *(second)* network for non-conforming clients is set up on the *(first)* telecommunication network and allows access to the session concentrator ;

the method comprises:

establishing a session between the non-conforming client and the session concentrator according to a point-to-point transport protocol on the *(second)* network for non-conforming clients;

transferring, by the session concentrator, the information transmitted by the non-conforming client in the established session to a *(third)* network for clients that conform to the access control protocol, the *(third)* network for conforming clients being set up on the *(first)* telecommunication network and allowing access to the services provided by the service provider, and reciprocally.

Contrary to the office action, there is nothing in Sobel et al. disclosing or suggesting two protocols (access control protocol and point-to-point transport protocol) or the relation of three communication networks (the second and third networks being set up on the first network).

A fortiori, Sobel et al. fails to disclose or suggest a *(second)* network for non-conforming clients established on the *(first)* telecommunication network, wherein such a (second) network allows the establishment of a session between at least one non-conforming client and the session concentrator according to the point-to-point transport protocol. There is nothing in Sobel et al. disclosing or suggesting a session concentrator transmitting client data to a *(third)* network for clients able to support the access protocol in order to allow the client access to services provided by the service provider.

Further Sobel et al. fails to disclose anything relating to "services", "service provider" or "session concentrator." In addition, the Sobel et al. goals and implementation are very different from those of the applicants' independent claims. Sobel et al. assigns clients a level of access to a protected network as a function of their compliance with the network's security policies. The method of claim 1 and the system

of claim 11 enable clients, <u>which are compliant with a point-to-point transport protocol</u>, to access services provided by a service provider even if these clients are not in compliance with the access control protocol enabling access to services of service providers.

The problem involving allowing a client compliant with a point-to-point transport to access a service provider using an access protocol to these services that is not liable to the establishment of PPP sessions is not discussed by Sobel et al.. As a consequence, Sobel et al. is not relevant to applicants' claims 1 and 11.

As a result of the arguments developed above, neither Hare et al nor Sobel et al. is relevant to applicants' independent claims since neither of them discloses the following features:

a _(second)_ <u>network for non-conforming clients</u> which is set up on the _(first)_ <u>telecommunication network</u> and allows access to the session concentrator;

establishing a session between the non-conforming client and the session concentrator <u>according to a point-to-point transport protocol</u> on the _(second)_ <u>network for non-conforming clients;</u>

transferring, by the session concentrator, the information transmitted by the non-conforming client in the established session to a _(third)_ <u>network</u> for clients that conform to the <u>access control protocol</u>, the _(third)_ <u>network</u> for conforming clients being set up on the _(first)_ <u>telecommunication network</u> and allowing access to the services provided by the service provider, and reciprocally.

A fortiori, the combination of Hare et al. and Sobel et al. is not relevant to the independent claims of the present patent application since neither of them discloses or suggests the aforesaid distinguishing essential features.

Consequentially dependent claims 2-10 and 12 of the present application are also new and unobvious at least because these claims depend on claim 1.

Malik is an instruction manual relating to computer network security. In this

reference, principles and practices of security for networks using IEEE 802.1x access control protocol are discussed. This manual further relates to implementing security policies and specific security tools to fight cyber-threats.

Malik does not disclose or suggest any technique for access by a client compliant with a point-to-point transport protocol to services provided by a service provider enabling such a client to access these services even if it is not compliant with the access protocol to these services. In other words, the problem of allowing a client compliant with a point-to-point transport to access a service provider using an access protocol to these services that is not liable to the establishment of PPP sessions is not found in Malik. Malik only concerns a manual for understanding and implementing a secured computer network. Thus, as implied from the office action Malik is not relevant to the independent claims of the present application.

Allowance is in order.

To the extent necessary, a petition for an extension of time under 37 C.F.R. 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 07-1337 and please credit any excess fees to such deposit account.

Respectfully submitted,

LOWE HAUPTMAN HAM & BERNER, LLP

/Allan M. Lowe/

Allan M. Lowe
Registration No. 19,641

1700 Diagonal Road, Suite 300
Alexandria, Virginia 22314
(703) 684-1111
(703) 518-5499 Facsimile
Date: November 12, 2009
AML/cjf